



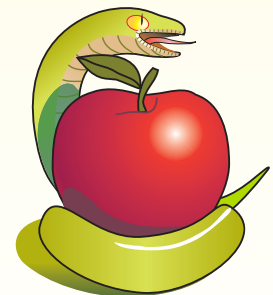
P.O.K. Protecting Our Kids



Preventing Your Child From Engaging in Online Crime

Concerned Web Parents can protect their kids by doing the following:

- n Talk to your children about the crimes kids can commit online, emphasizing that such crimes are prosecuted and are accompanied by jail time and/or probation. A criminal record for a juvenile can be a life-altering experience, especially for those who may be applying to college or military academies.
- n Keep the computer in a family room so that you can monitor the Internet use. Tell your children that you have the right to monitor their computer use and that if you suspect there is a problem, you will randomly monitor their Internet activities.
- n Install an operating system that makes you the administrator, for example, Windows XP or Mac OS X. Create a password that will allow only you to control the computer's Internet settings, online content, and the software that can be installed. This is a very important step in monitoring your child's online activities, even when you are away from the home. If you are unable to establish yourself as your computer's administrator, then someone else has been designated as the administrator. If the administrator is your child, you can regain control of your computer through your child's user ID and password. Once you become the new administrator, you can control the Internet content and Web sites your child has access to. For more detailed information visit the D.A.'s website.
- n Do not allow your child to have multiple e-mail accounts or create accounts without your knowledge. Insist that your children give you their e-mail and chat passwords. Internet accounts and primary screen names should be in your name.
- n Go online with your kids and find out who they chat with and prohibit the use of private chat rooms with people they don't know personally. Ask them about the people that are on their contact and/or buddy list.
- n Tell your child to let you know immediately if a stranger tries to make contact with them on the Web, whether through an Instant Message, chat room, or e-mail. The stranger may be an adult pretending to be a child, or an Internet con artist looking to recruit kids to do his online dirty work.
- n Tell your children they are not allowed to purchase or sell anything on the Internet without your consent. Nor may they create an auction house account because they are minors, and the law prohibits them from doing so.
- n Make sure your child knows never to divulge any personal information on the Internet, including his or her name, age, photos, gender, physical





P.O.K. Protecting Our Kids



description, hobbies (especially illegal ones such as hacking, pirating, etc.), telephone number, address, etc. The Internet is a place where children can quickly be recruited to join fraudulent auction house rings, hacker clubs, and other criminal syndicates.

- n Set rules as to what sites your children are allowed to visit and which ones they are not. Be on the lookout for sites where kids can go to illegally download software, and watch for "hacking" sites that teach people how to infiltrate business and government computer systems.

- n Set time limits on their computer use. Children who spend substantially more time in front of the computer than they do interacting with their friends in person or on the phone may be prone to take part in criminal online activity. Do not let your children's Internet identity define who they are. Kids need real world social outlets.

- n Do not allow your children to chat (send Instant Messages) while doing homework.

- n Consider purchasing third-party filtering software such as Cyberpatrol or NetNanny. You should be able to find software that meets your needs at most software electronics stores.

- n Become familiar with the Web browser your kids use, and restrict the type of content (violence, sex, and language) that can be viewed.